ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1), 21 U.S.C. § 844(a), and 18 U.S.C. § 1343 including:

A. Records and tangible objects pertaining to the following topics:

1. controlled substances, including but not limited to GHB, drug packaging material, and related paraphernalia;
2. any scheme or artifice to defraud involving fraudulent money orders, as well as communications about any such scheme; and
3. communications with any undercover agent(s) of the Federal Bureau of Investigation between March - July 2020, or any records or objects relating to or referencing such communications or such agent(s);

B. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;
2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of when the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage;

C. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rental or lease agreements, rent payments, mortgage bills and/or payments, photographs, insurance documentation, receipts, and check registers); and

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, mobile phone, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable

storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or

instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.